IN THE CLAIMS

Please amend the claims to read as follows:

Listing of Claims

1-61. (Canceled).

62. (New) A data processing system for generating a key protection certificate comprising:

a Personal Security Device (PSD) comprising a unique device name, a cryptography section, a data processing section, a data storage section and a communications section,

wherein said cryptography section includes an asymmetric cryptographic key pair generating algorithm, a first securely shared secret key, a symmetric cryptography section, a concatenation algorithm, a message authentication code algorithm, cryptographic seed information, and a key protection certificate generating algorithm, and

wherein said key protection certificate generating algorithm produces conditionally with said asymmetric cryptographic key pair generating algorithm, upon completion by said PSD of said asymmetric cryptographic key pair generation and in dependence on said generated asymmetric cryptographic key pair, a unique digital certificate that comprises a proof of possession by said

PSD of said first securely shared secret key and of said asymmetric cryptographic key pair generated by said PSD.

63. (New) The system according to claim 62, wherein at least a portion of said cryptographic seed information is used by said asymmetric key pair generating algorithm to generate at least one asymmetric private key and one asymmetric public key upon receipt of at least one key generation command, said keys being stored in a secure domain of said PSD.

64. (New) The system according to claim 63, wherein said key protection certificate generating algorithm, upon receipt of said key generation command, generates a plurality of contextual attributes.

65. (New) The system according to claim 64, wherein at least a portion of said contextual attributes are encrypted using said first shared secret key and said symmetric cryptography section to generate private contextual attributes.

66. (New) The system according to claim 65, wherein the remaining unencrypted of said plurality of said contextual attributes forms public contextual attributes.

67. (New) The system according to claim 66, wherein a signed device name is generated using said unique device name and said asymmetric private key as inputs into said signing algorithm.

68. (New) The system according to claim 67, wherein said private contextual attributes, public contextual attributes, signed device name and unique device name are concatenated by said concatenation algorithm, generating a first intermediate result.

69. (New) The system according to claim 68, wherein a message authentication code is generated using a second securely shared secret key and said first intermediate result as inputs into said message authentication code algorithm, forming a second intermediate result.

70. (New) The system according to claim 69, wherein said first intermediate result and said second intermediate result are concatenated by said concatenation algorithm forming said key protection certificate then stored in said secure domain of said PSD.

71. (New) The system according to claim 62, wherein said unique device name is an embedded serial number.

72. (New) The system according to claim 71, wherein said unique device name is the result of a cryptographic process using said embedded serial number as a cryptographic seed.

73. (New) The system according to claim 62, wherein said communications section includes a receiving section that receives commands to generate asymmetric and symmetric keys and a sending section that sends said public key and said key protection certificate.

74. (New) A data processing system for validating a key protection certificate generated by a Personal Security Device (PSD) comprising:

a data processing section, a data storage section, a communications section, a cryptography section, a first securely shared secret key and a public key,

wherein said cryptography section includes a message authentication code algorithm, a cross referencing section and a comparator algorithm, and wherein said cross referencing section comprises a selection section that selects proper first securely shared secret keys, a proper public key, proper cryptography algorithms and reference parameters associated with said key protection certificate, by use of a unique device name of said PSD contained in said key protection certificate.

75. (New) The system according to claim 74, wherein said proper first securely shared secret key and said public key have a direct generation relationship with said key protection certificate.

76. (New) The system according to claim 74, wherein said communications section includes a request transmitting section that transmits requests for said key protection certificate and a receiving section that receives said key protection certificate.

77. (New) The system according to claim 76, wherein said received key protection certificate includes private contextual attributes, public contextual attributes, said unique device name of said PSD, a signed device name and a message authentication code in dependence on said private contextual attributes, said

public contextual attributes, said unique device name of the PSD, and said signed device name.

78. (New) The system according to claim 76, wherein said signed device name is decrypted using said proper public key, generating a second device name.

79. (New) The system according to claim 78, wherein said second device name and said unique device name of said PSD contained in said certificate are compared by the comparator algorithm to determine if said second device name and said unique device name of said PSD contained in said certificate match.

80. (New) The system according to claim 76, wherein a second message authentication code is generated using said private contextual attributes, said public contextual attributes, said unique device name of said PSD, said signed device name included in said certificate and a proper second securely shared secret key as inputs into said message authentication code algorithm.

81. (New) The system according to claim 80, wherein said second message authentication code and said message

authentication code contained in said certificate are compared using said comparator algorithm to determine if said second message authentication code and said message authentication code contained in said certificate match.

82. (New) The system according to claim 76, wherein said private contextual attributes are decrypted using said proper first securely shared secret key.

83. (New) The system according to claim 82, wherein at least one predetermined parameter is contained in at least a portion of said decrypted private contextual attributes.

84. (New) The system according to claim 83, wherein at least one predetermined parameter and said reference parameters are compared using said comparator algorithm to determine if said at least one predetermined parameter and said reference parameters match.

85. (New) The system according to claim 79, 81 or 84, wherein a failure to achieve a match invalidates said key protection certificate.

86. (New) A method for generating a key protection certificate comprising:

injecting a first securely shared secret key, a second securely shared secret key, a key protection algorithm and cryptographic seed information into a PSD which comprises a unique device name, wherein at least a portion of said seed information is used in generating at least one public key and one private key,

storing said injected first and second securely shared secret keys and said cryptographic seed information in a secure domain within said PSD,

sending a command to said PSD for generating said at least one public key and one private key, wherein said command initiates generation of said keys and of said key protection certificate,

generating said at least one public key and said one private key using at least a portion of said seed information,

generating contextual attributes specific to at least the generation of said private key,

encrypting at least a portion of said contextual attributes using said first securely shared secret key, forming private contextual attributes and public contextual attributes, wherein predetermined parameters are included in said private contextual attributes,

storing said public key and said private key in said secure domain within said PSD,

generating a digital signature of said unique device name using said private key,

concatenating said unique device name, said private contextual attributes, said public contextual attributes with said digital signature and generating a first intermediate result,

generating a message authentication code of said first intermediate result using said second securely shared secret key producing a second intermediate result,

concatenating said first intermediate result with said second intermediate result producing said key protection certificate; and

storing said key protection certificate in said secure domain within said PSD.

87. (New) A method for validating a key protection certificate generated by a PSD comprising:

receiving said key protection certificate, wherein said certificate contains at least a plain text device name portion, a signed device name portion and cryptogram portion,

cross-referencing said device name with proper first and second securely shared secret keys, a proper public key, proper cryptographic algorithms and reference parameters associated with said key protection certificate,

verifying said signed device name portion of said certificate using said proper public key,

comparing the resulting device name with said device name portion included in said certificate,

independently performing a message authentication code function on said concatenated private contextual attributes, public contextual attributes, device name, and signed device name portions of said certificate using a first of said proper securely shared secret keys,

comparing the resulting message authentication code with a method authentication code included in said certificate,

decrypting said private contextual attributes using a second of said proper securely shared secret keys,

comparing at least a portion of the private contextual attributes to the reference parameters, validating said certificate if said resulting device name matches said device name contained in said certificate, said independently generated message authentication code matches said message authentication code contained in said certificate and at least a portion of said private contextual attributes matches said reference parameters,

rejecting said certificate if any of said matches is not achieved.

88. (New) The method according to claim 87, wherein said receiving party possesses said proper securely shared secret keys and said proper public key.

89. (New) The method according to claim 88, wherein said receiving party is a trusted third party certificate authority.

90. (New) A data processing system for generating a key protection certificate comprising a Personal Security Device (PSD) further comprising a unique device name, at least one asymmetric cryptographic key pair generating algorithm, a first securely shared secret key, a key protection certificate generating algorithm, a data processing section, a data storage section and a communications section, wherein said key protection

certificate generating algorithm produces conditionally with said asymmetric cryptographic key pair generating algorithm, upon completion by said PSD of said asymmetric cryptographic key pair generation and in dependence on said generated asymmetric cryptographic key pair, a unique digital certificate that comprises a proof of possession by said PSD of said first securely shared secret key and of said asymmetric cryptographic key pair generated by said PSD.

91. (New) A data processing system for validating a key protection certificate generated by a Personal Security Device (PSD) comprising a data processing section, a data storage section, a communications section, a cryptography section, at least one cryptographic key, and a cross referencing section, wherein cross referencing section comprises a selection section that selects at least one proper cryptographic key and one proper cryptography algorithm associated with said key protection certificate, by use of a unique device name of said PSD contained in said key protection certificate.

92. (New) A method for generating a key protection certificate comprising sending a command to a Personal Security Device (PSD) comprising a unique device name and a first securely

shared secret key for generating at least one asymmetric cryptographic key pair, wherein said command initiates generation by said PSD of said asymmetric cryptographic key pair and of said key protection certificate that comprises a proof of possession by said PSD of said first securely shared secret key and of said asymmetric cryptographic key pair generated by said PSD.

93. (New) A method for validating a key protection certificate generated by a Personal Security Device (PSD) comprising:

receiving said key protection certificate, wherein said certificate contains at least a unique device name of said PSD,

cross-referencing said device name with at least one proper cryptographic key and one proper cryptography algorithm associated with said key protection certificate, and

validating said key protection certificate with at least said proper cryptographic key and said proper cryptography algorithm.

94. (New) A computer program product embodied in a tangible form having instructions executable by said PSD to at least implement the method of claim 86.

95. (New) A computer program product embodied in a tangible form having instructions executable by said PSD to at least implement the method of claim 92.

96. (New) A computer program product embodied in a tangible form having instructions executable by said data processing system to at least implement the method of claim 87.

97. (New) A computer program product embodied in a tangible form having instructions executable by said data processing system to at least implement the method of claim 93.